# Damien ROBERT

*Researcher in cryptography*

*Inria Bordeaux Sud-Ouest*

*Libourne, France*
*+33 (0)6 66 56 25 49*
*+33 (0)5 40 00 21 56*
*damien.robert@inria.fr*
*www.normalesup.org/~robert/*
*DamienRobert*
*French, Born in 1984*


## Research

List of publications: *www.normalesup.org/~robert/pro/publications/* , see also *the appendix*.

## Work

March 2012–Present **Researcher**, *Inria Bordeaux Sud-Ouest, Bordeaux*, Inria Team LFANT
Elliptic curves, abelian varieties and algorithmic number theory applied to cryptography

August 2011–February 2012 **Researcher Engineer**, *Microsoft Research, Redmond*, Team manager: Kristin Lauter
Developing the Microsoft cryptographic library.

October 2010–August 2011 **Postdoc**, *Inria Bordeaux Sud-Ouest, Bordeaux*, Team manager: Andreas Enge
Genus 2 curves and complex multiplication.

July 2010–September 2010 **Microsoft Research Summer Internship**, *Redmond, USA*, Mentor: Kristin Lauter
Speeding up the CRT method in genus 2 for generating class polynomials

## Education

January 2007–June 2010 **PhD Thesis**, *University Henri Poincaré and Loria, Nancy*, Advisor: Guillaume Hanrot, Teaching Fellow (Moniteur) in Computer Science
Theta functions and applications in cryptography. Defended July 23 2010.

September–December 2006 **Master of Science in Computer Science**, *Paris*, Master Parisien de Recherche Informatique, (Inscription Pédagogique)
Courses in cryptography and algebraic number theory

2004–2006 **Master of Science in Mathematics**, *Paris VI, Paris VII, Paris XI, École Polytechnique*, Algebra and Geometry, With Honors (Courses: 19.88/20, Master Thesis: 18/20, Total: 18.94/20)
(Pedagogic inscription in 2004–2005.) Master Thesis on "Classification of complex reflexion groups", Advisor: Michel Broué (Institut Henri Poincaré).

2004–2005 **Agrégation in Mathematics**, Nationwide competitive examination for recruiting teachers for undergraduate students, Rank 9

2003–2007 **École Normale Supérieure**, *Paris*, Computer Science, Admitted after the French "Grandes Écoles" competitive examination, Rank 1

2003–2006 **Magistère in Mathematics (MMFAI)**, With Honors

2003–2004 **Bachelor of Science in Mathematics (L3–M1)**, With Honors (L3: 19/20, M1 Courses: 18.67/20, M1 Thesis: 14/20, M1 Total: 17/20)
Minor in Computer Science. Bachelor Thesis on « Clifford modules and $K$-theory », with Mehdi Tibouchi, advisor François Pierrot.

## Experiences

2003 – 2006 Computer Tutor. Help students to use the school computers, organizations of workgroup on LaTeX, Unix..., École Normale Supérieure, Paris.

2003 – 2006 Student administrator. Help the system administrators to maintain the school computers (on Solaris and FreeBSD), configuration of the user sessions, software installation, École Normale Supérieure, Paris.

## Langages

French Native Speaker

English Fluent *I have lived one year in Knoxville, Tennessee*

German Basic

## Technical Skills

Programing C, Java, Ocaml, Perl, PHP, Ruby, Shell

Scientific Magma, Matlab, Pari, Sage

Web (X)HTML, CSS, Javascript

OS Linux (Archlinux)

VCS Git, Mercurial, Subversion

Typography LuaLaTeX

## Hobbies

Sport Juggling, Rock Climbing, Tennis.

Safety French First Aid Certificate

Other Driving license.

# Scientific activities

## Publications

- D. Robert. "Breaking SIDH in polynomial time". Apr. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/breaking_sidh.pdf. eprint: 2022/1038, HAL: hal-03943959, Slides: 2023-04-Eurocrypt.pdf (15 min, Eurocrypt 2023, April 2023, Lyon, France).
- D. Lubicz and D. Robert. "Fast change of level and applications to isogenies". In: *Research in Number Theory (ANTS XV Conference)* 9.1 (Dec. 2022). DOI: 10.1007/s40993-022-00407-9. URL: http://www.normalesup.org/~robert/pro/publications/articles/change_level.pdf. HAL: hal-03738315.
- A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". In: *Moscow Mathematical Journal* 22 (Feb. 2022), pp. 613–655. URL: http://www.normalesup.org/~robert/pro/publications/articles/cyclic.pdf. HAL: hal-01629829.
- M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. "Spanning the isogeny class of a power of an elliptic curve". In: *Mathematics of Computation* 91.333 (Sept. 2021), pp. 401–449. DOI: 10.1090/mcom/3672. arXiv: 2004.08315. URL: http://www.normalesup.org/~robert/pro/publications/articles/algebraic_obstruction.pdf. HAL: hal-02554714.
- A. Maiga and D. Robert. "Computing the 2-adic canonical lift of genus 2 curves". In: *Proceedings of the Seventh International Conference on Mathematics and Computing – ICMC 2021*. Ed. by D. Giri, K.-K. R. Choo, S. Ponnusamy, W. Meng, S. Akleylek, and S. P. Maity. Vol. 1412. Advances in Intelligent Systems and Computing (ICMC 2021). Singapore: Springer, Mar. 2022, pp. 637–672. DOI: 10.1007/978-981-16-6890-6_48. URL: http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2_p2.pdf. HAL: hal-03119147.
- E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". In: *Journal of Number Theory* 216 (Nov. 2020), pp. 403–459. DOI: 10.1016/j.jnt.2020.04.014. URL: https://www.sciencedirect.com/science/article/abs/pii/S0022314X20301402. HAL: hal-01520262, Reproducible archive: https://data.mendeley.com/datasets/yy3bty5ktk/1.
- D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (May 2016), pp. 130–158. DOI: 10.1016/j.ffa.2016.01.009. URL: http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf. HAL: hal-01057467, eprint: 2014/493.
- D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS Journal of Computation and Mathematics* 18 (1 Feb. 2015), pp. 198–216. DOI: 10.1112/S146115701400045X. arXiv: 1402.3628. URL: http://www.normalesup.org/~robert/pro/publications/articles/rational.pdf. HAL: hal-00954895.
- D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: *Journal of Symbolic Computation* 67 (Mar. 2015), pp. 68–92. DOI: 10.1016/j.jsc.2014.08.001. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192.
- R. Cosset and D. Robert. "An algorithm for computing $(\ell, \ell)$-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". In: *Mathematics of Computation* 84.294 (Nov. 2015), pp. 1953–1975. DOI: 10.1090/S0025-5718-2014-02899-8. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143.

- K. E. Lauter and D. Robert. "Improved CRT Algorithm for Class Polynomials in Genus 2". In: *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. Berkeley: Mathematical Sciences Publisher, Nov. 2013, pp. 437–461. DOI: 10.2140/obs.2013.1.437. URL: http://www.normalesup.org/~robert/pro/publications/articles/classCRT.pdf. Slides: 2012-07-ANTS-SanDiego.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-X), July 2012, San Diego, USA), HAL: hal-00734450, eprint: 2012/443.
- D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compositio Mathematica* 148.5 (Sept. 2012), pp. 1483–1515. DOI: 10.1112/S0010437X12000243. arXiv: 1001.2016 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf. HAL: hal-00446062.
- J.-C. Faugère, D. Lubicz, and D. Robert. "Computing modular correspondences for abelian varieties". In: *Journal of Algebra* 343.1 (Oct. 2011), pp. 248–277. DOI: 10.1016/j.jalgebra.2011.06.031. arXiv: 0910.4668 [cs.SC]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf. HAL: hal-00426338.
- D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: ed. by G. Hanrot, F. Morain, and E. Thomé. Vol. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer–Verlag, July 2010. DOI: 10.1007/978-3-642-14518-6_21. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides: 2010-07-ANTS-Nancy.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-IX), July 2010, Nancy), HAL: hal-00528944.

## Preprints

- P. Dartois, L. Maino, G. Pope, and D. Robert. "An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography". Nov. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/_2_2__isogenies_in_the_theta_model.pdf
- P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. "SQISignHD: New Dimensions in Cryptography". Mar. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/SQISignHD.pdf. eprint: 2023/436.
- D. Robert. "The geometric interpretation of the Tate pairing and its applications". Feb. 2023. URL: http://www.normalesup.org/~robert/pro/publications/articles/geometric_tate_pairing.pdf. eprint: 2023/177.
- D. Robert. "Some applications of higher dimensional isogenies to elliptic curves (overview of results)". Dec. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies_applications.pdf. eprint: 2022/1704, HAL: hal-03943973.
- D. Robert. "Evaluating isogenies in polylogarithmic time". Aug. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/polylog_isogenies.pdf. eprint: 2022/1068, HAL: hal-03943970.
- A. Maiga and D. Robert. "Towards computing canonical lifts of ordinary elliptic curves in medium characteristic". Mar. 2022. URL: http://www.normalesup.org/~robert/pro/publications/articles/fast_canonical_lift_g1.pdf. HAL: hal-03702658.
- A. Maiga and D. Robert. "Computing the canonical lift of genus 2 curves in odd characteristic". Dec. 2020. URL: http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf. HAL: hal-03738314.

- D. Lubicz and D. Robert. "Linear representation of endomorphisms of Kummer varieties". Dec. 2020. URL: http://www.normalesup.org/~robert/pro/publications/articles/action.pdf. HAL: hal-03204365.
- J. Kieffer, A. Page, and D. Robert. "Computing isogenies from modular equations between Jacobians of genus 2 curves". Oct. 2020. arXiv: 2001.04137 [math.AG]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular_isogenies_g2.pdf. HAL: hal-02436133.

## Reports

- Andreas Enge, Damien Robert, Computing class polynomials in genus 2. DGA Report, April 2013.

## Books

- Damien Robert, General theory of abelian varieties and their moduli spaces. March 2021. Draft version.
- Guide to Pairing-Based Cryptography. 2017. Chapter 3 on « Pairings » with Sorina Ionica, and Chapter 10 on « Choosing Parameters » with Sylvain Duquesne, Nadia El Mrabet, Safia Haloui and Franck Rondepierre

## HDR

- Efficient algorithms for abelian varieties and their moduli spaces. Habilitation à diriger les recherches, June 2021, Université Bordeaux. (Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux), Detailed version.)

## PhD Thesis

- Theta functions and cryptographic applications (in French). PhD thesis in Computer Sciences, July 2010, Université Henri-Poincarré, Nancy. (Slides: 2010-07-Phd-Nancy.pdf (1h, Nancy), TEL: tel-00528942.)

## Prizes

February 2012 — Received the second prize in Science for the Lorraine Region PhD awards, Metz. (Inria announcement)

October 2011 — Received the Lorraine University PhD awards in the domain of IAEM (Computer science, Mathematics, Electronic), Nancy. (Photos of the ceremony)

## Softwares

- AVIsogenies (Abelian Varieties and Isogenies), with Gaëtan Bisson, Romain Cosset. Magma package devoted to the computation of isogenies between abelian varieties, 2010. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.000.10000). Latest version 0.7, released on 2021-03-13.
- FromLatticesToModularForms. Computation of modular forms in the isogeny class spanned by products of elliptic curves, April 2020.
- ThetaIsogenies. Fast computations of isogenies in dimension two, November 2023.

## Teaching

2016 – Present — Elliptic curves. Master 2 Cryptologie et Sécurité Informatique and Master AGTN/Algant ALgebra, Geometry and Number Theory, Université Bordeaux. Exercices, Master CSI, Master Algant

January 2020 — Probability for Capes. Master 2 Enseignement, Université de la Polynésie Française. Formulaires

September 2017 — SIDH. Course on SIDH for the kick-off meeting of the Lirima Team FAST, Institut de Mathématiques de Bordeaux.

June 2017 — Elliptic Curves and Cryptography. Mini Course for the Jury of Agregation de Mathématiques, Lille.

2016 — Elliptic curves. Master 1 Cryptologie et Sécurité Informatique, Université Bordeaux. Master CSI

December 2015 — Introduction to cryptology. Seminar on security of the Colloque de Recherche en Informatique (CRI 2015), Université Yaoundé I, Cameroun. À quoi sert la cryptologie? Petit panorama des mathématiques de la cryptologie, Introduction to cryptology: confidentiality, integrity, authenticity, Modern cryptology: from public key cryptography to homomorphic encryption

September 2015 — The group structure of rational points of elliptic curves over a finite field (3h). Elliptic Curves Cryptography (ECC 2015) Summer School, Bordeaux. (Exercices.)

March 2015 — Algorithmic number theory and cryptology. One week courses for the École Mathématique Africaine, organised with support from the Centre International de Mathématiques Pures et Appliquées (CIMPA), Franceville, Gabon. Introduction to the course, Slides, Examples (X509, ssh, gpg)

September 2011 — Isogenies and endomorphism rings of elliptic curves (2h30). ECC 2011 Summer School, Nancy.

2007 – 2010 — Teaching Fellow (Moniteur) in Computer Science. Université Henri-Poincaré (Nancy).
- Tutorials of the cryptography course (M1, 30h).
- Course on Web technologies: HTML, CSS, PHP and MySQL (L1, 60h).
- Tutorials of the OCaml programming course (L1, 120h).

March 2004 – May 2004 — Corps quadratiques et groupes de classes. Workgroup organized with Mehdi Tibouchi, École Normale Supérieure, Paris.

## Students

2023 – 2024 — Sabrina Kunzweiler. Postdoc ANR Ciao, Inria Bordeaux Sud-Ouest.

2022 – Present — Pierrick Dartois, Security analysis and improvement of isogeny based post-quantum cryptosystems, cosupervising with Luca de Feo, Benjamin Wesolowski. Phd Thesis, Institut de Mathématiques de Bordeaux.

2022 – Present — Nicolas Sarkis, Decomposable abelian surfaces and applications to HECM, cosupervising with Razvan Barbulescu. Phd Thesis, Institut de Mathématiques de Bordeaux.

2020 — Oren Nezer, Verifiable Delayed Functions. Master, Institut de Mathématiques de Bordeaux.

September 2018 – July 2021 — Jean Kieffer, Higher-dimensional modular equations, applications to isogeny computations and point counting, cosupervising with Aurel Page. Phd Thesis, Institut de Mathématiques de Bordeaux.

2016 – June 2022 — Abdoulaye Maiga, Canonical lift of abelian surfaces, cosupervising with Djiby Sow. Phd Thesis, Cheikh Anta Diop, Sénégal.

2018 — Antton Domercq, Rémi Clarisse, Supersingular isogeny Diffie-Hellman. Projet de deuxième année.

2017 — Margarita Pierrackea, Supersingular isogeny key-exchange. Master, Institut de Mathématiques de Bordeaux.

2016 — Liu Zhengying, Height of class polynomials. Stage 3A École Polytechnique, Institut de Mathématiques de Bordeaux.

2015 – 2016 Cyril Bouvier, cosupervising with Guilhem Castagnos. Postdoc ANR SIMPATIC, Institut de Mathématiques de Bordeaux.

2014 – 2015 Sorina Ionica, cosupervising with Guilhem Castagnos. Postdoc ANR SIMPATIC, Institut de Mathématiques de Bordeaux.

November 2012 – December 2015 Enea Milio, Computing modular polynomials in dimension 2, cosupervising with Andreas Enge. Phd Thesis, Inria Bordeaux Sud-Ouest.

2014 Illaria Chillotti, Pairings over elliptic curves using isogenies. Master, Institut de Mathématiques de Bordeaux.

2013 Giulio Di Piazza, Arithmetic on Jacobians of algebraic curves. Master, Institut de Mathématiques de Bordeaux.

2012 Ilaria Lovato, Computing Modular Polynomials with Theta Functions, cosupervising with Andreas Enge. Master, Institut de Mathématiques de Bordeaux.

## Responsibilities

2023 Leader of the team Canari (Cryptography, ANalysis and ARIthmetic). Inria Bordeaux Project Team.

2019 – 2023 Leader of the ANR Ciao (Cryptography, isogenies and abelian varieties overwhelming).

2018 – Present Chargé de mission Développement logiciel, Institut Mathématiques de Bordeaux.

2016 – 2019 FAST. Director of the team FAST, inside the laboratory LIRIMA.

2014 – 2020 Jury of Mathematics agregation competition.
- Leader of Option C Algèbre et Calcul Formel since 2016

December 2015 – Present Commission Consultative 25, Institut Mathématiques de Bordeaux.

January 2015 – September 2018 Commission Jeunes Chercheurs, Inria Bordeaux.

June 2013 – 2016 MACISA. Codirector of the team MACISA, inside the laboratory LIRIMA (Since September 2014; previously scientific adviser for the theme "Elliptic and hyperelliptic curves cryptography").

October 2010 – September 2019 Organisation of the LFANT seminars.

2012 – 2016 Member of the ERC Antics (Algorithmic Number Theory in Computer Science).

2013 – 2016 Member of the Industrial ANR Simpatic (SIM and PAiring Theory for Information and Communications security).

2012 – 2015 Member of the ANR Peace (Parameter spaces for Efficient Arithmetic and Curve security Evaluation).

2012 – Present Member of the LabEx CPU (Numerical certification and reliability).

2009 – 2012 Member of the ANR Chic (Hyperelliptic curves, isogenies and point counting).

## Comitees

December 2018 ANTS XIII, University of Wisconsin, Madison. Scientific Comitee.

December 2015 CRI 2015, Yaoundé, Cameroun. Scientific Comitee.

December 2015 Asiacrypt 2015, Auckland. Scientific Comitee.

September 2015 Elliptic Curves Cryptography (ECC 2015), Bordeaux. Organisation Comitee, Scientific Comitee.

August 2013 Selected Area in Cryptography (SAC 2013), Simon Fraser University, Canada. Scientific Comitee.

## Invited Speaker

- Arithmetic and pairings on Kummer lines (45min). Leuven isogeny days 4, October 2023, Leuven.
- Efficient representation of isogenies (1h). EWHA-KMS International Workshop on Cryptography, July 2023.
- Applications of isogenies between abelian varieties to elliptic curves (1h). Arithmétique en Plat Pays, March 2023.
- Applications of isogenies between abelian varieties to elliptic curves cryptosystems (1h). Vantage Seminar, December 2022.
- Isogenies between abelian varieties – an algorithmic survey (1h). Leuven isogeny days 3, September 2022, Leuven.
- Isogenies, Polarisations and Real Multiplication (1h). Journées C2 Codage et Cryptographie, October 2015, La Londe-Les-Maures.
- Isogenies, Polarisations and Real Multiplication (1h). Modular Forms and Curves of Low Genus: Computational Aspects, September 2015, ICERM, Providence, USA. (Long version.)
- Optimal pairings on abelian varieties (1h). Elliptic Curves Cryptography (ECC 2014), October 2014, Chennai, India.
- Isogenies between abelian varieties (Notes) (1h). ANR Peace conference Effective moduli spaces and applications to cryptography, June 2014, Rennes.
- Pairings on abelian varieties and the Discrete Logarithm Problem (1h). Discrete Logarithm Problem Conference DLP 2014, May 2014, Ascona, Suisse.
- Computing optimal pairings on abelian varieties with theta functions (1h). Geometry and Cryptography (Geocrypt 2011), June 2011, Bastia.
- Generalizing Vélu's formulas and some applications (1h). Elliptic Curves Cryptography (ECC 2010), 25 year anniversary of elliptic curves computation, October 2010, Redmond, USA. (Video link.)
- A Vélu's like formula for computing isogenies on Abelian Varieties (1h). Conférence Algorithmique et Arithmétique avec applications à la cryptographie, May 2010, Moscow, Russia.

## Talks

- New applications of higher dimensional isogenies (1h). Loria, Nancy, September 2023.
- Breaking SIDH in polynomial time (1h). Institut Fourier, Grenoble, April 2023.
- Applications of isogenies between abelian varieties to elliptic curves (1h). LFANT Seminar, March 2023. On blackboard
- The geometric interpretation of the Tate pairing (1h). ANR Ciao Workshop, December 2022. On blackboard
- Evaluating isogenies in polylogarithmic time (1h). LFANT Seminar, October 2022. On blackboard
- Breaking SIDH in polynomial time (1h). LFANT Seminar, September 2022, Bordeaux.
- Towards computing the canonical lift of an ordinary elliptic curve in medium characteristic (1h). LFANT Seminar, April 2022, Bordeaux. On blackboard

- Revisiter l'algorithme de Satoh de comptage de points en petite caractéristique par relèvement canonique (1h). LFANT Seminar, October 2021, Bordeaux. On blackboard
- Calcul d'isogénies sur des variétés abéliennes (1h). CIAO Kickoff Meeting, February 2020, Bordeaux. On blackboard
- Extending Elkies' isogeny algorithm to genus 2 (1h). GAATI team, January 2020, Tahiti. On blackboard
- An overview of isogenies computations (1h). LFANT Seminar, September 2019, Bordeaux. On blackboard
- Modular Polynomials (1h). LIRIMA Team FAST kick-off conference, September 2017, Bordeaux. On blackboard
- Arithmetic on Abelian and Kummer varieties (2x1h). INRIA Team LFANT seminar, May 2015, Bordeaux. On blackboard, notes.
- Arithmetic on Elliptic Curves, Abelian varieties and Kummer varieties (45min). École Mathématique Africaine, March 2015, Université de Masuku, Franceville, Gabon.
- Arithmetic on Abelian and Kummer varieties (1h). Number Theory Seminar, December 2014, Caen. On blackboard, notes.
- Isogeny graphs in dimension 2 (1h). Cryptography Seminar, December 2014, Caen.
- Arithmetic on Abelian and Kummer varieties (1h). Number Theory Seminar, April 2014, Institut Fourier, Grenoble. On blackboard, notes.
- Arithmetic on abelian varieties and related topics (1h). Seminar in Coding Theory and Cryptography of the University of Zurich and the University of Neuchâtel, March 2014, Neuchâtel, Suisse.
- Computing optimal pairings on abelian varieties with theta functions (1h). Industrial ANR Simpatic meeting, January 2014, Caen.
- Arithmetic on Abelian and Kummer varieties (30min). ANR Peace meeting, December 2013, Rennes.
- On isogenies and polarisations (1h). LFANT Seminar, November 2013, Bordeaux.
- On isogenies and polarisations (30min). Geometry and Cryptography (Geocrypt 2013), October 2013, Tahiti.
- On isogenies between abelian varieties (45min). Microsoft Research, August 2013, Redmond, USA.
- Computing optimal pairings on abelian varieties with theta functions (1h). Microsoft Research, August 2013, Redmond, USA.
- Computing optimal pairings on abelian varieties with theta functions (30min). Arithmetic Geometry Cryptography and Coding Theory (AGCT 14), June 2013, Luminy, Marseille.
- Computing optimal pairings on abelian varieties with theta functions (1h). Lacal, May 2013, Lausanne.
- Computing optimal pairings on abelian varieties with theta functions (1h). CCIS seminar, April 2013, Grenoble.
- Computing cyclic isogenies using real multiplication (Notes) (1h). ANR Peace meeting, April 2013, Paris.
- Computing rational isogenies from the equations of the kernel (30min). ANR Peace meeting, November 2012, Paris.
- Improved CRT Algorithm for class polynomials in genus 2 (1h). Microsoft Research, August 2012, Redmond, USA.
- About the CRT method to compute class polynomials in dimension 2 (1h). INRIA Team LFANT seminar, May 2012, Bordeaux.

- Algorithms on abelian varieties for cryptography (1h). Caen's Cryptographic Seminar, March 2012, Caen.
- Algorithms on abelian varieties for cryptography (2h). INRIA Team Grace Seminar, January 2012, LIX, École Polytechnique, Paris.
- Algorithms on abelian varieties for cryptography (1h). B□utte aux caillesS□eminar, January 2012, Télécom ParisTech, Paris.
- Public key cryptography with abelian varieties: results and challenges (1h). ARITH Seminar, November 2011, Montpellier.
- Computing optimal pairings on abelian varieties with theta functions (1h). Séminaire de théorie des nombres, September 2011, Bordeaux.
- About the CRT method to compute class polynomials in dimension 2 (1h). Journées C2 Codage et Cryptographie, April 2011, Oléron.
- Cryptology, elliptic curves and number theory (1h). Number Theory PhD Students' seminar, March 2011, Bordeaux.
- Computing optimal pairings on abelian varieties with theta functions (1h). Séminaire Arithmétique et Théorie de l'Information, February 2011, Université Méditerranée, Marseille.
- Abelian varieties, theta functions and cryptography (1h30). PhD Students' seminar, February 2011, Université Méditerranée, Marseille.
- Computing isogenies and applications in cryptography (1h). Cryptology seminar, January 2011, Université Versailles Saint-Quentin, Versailles.
- Computing isogenies and applications in cryptography (1h). Minalogic cryptology seminar, January 2011, Grenoble.
- Abelian varieties, theta functions and cryptography (40min+40min). Algorithmics of L-functions workshop, December 2010, Bordeaux. Part 1 on blackboard.
- On the CRT method to compute class polynomials in genus 2 (30min). ANR Chic, December 2010, Paris.
- Generalizing Vélu's formulas and some applications (1h). TANC Seminar, November 2010, LIX, École Polytechnique, Paris.
- Speeding up the CRT method to compute class polynomials in genus 2 (1h). Microsoft Research, September 2010, Redmond, USA.
- Abelian varieties, Theta functions and cryptography (30min). Microsoft Research, July 2010, Redmond, USA.
- Arithmétique rapide avec les fonctions thêta (20min). ANR Chic, June 2010, Paris.
- A Vélu's like formula for computing isogenies on abelian varieties (1h). Séminaire de théorie des nombres, February 2010, Bordeaux.
- Calcul de pairing avec les fonctions thêta (1h). LFANT Cryptographic Seminar, February 2010, Bordeaux.
- A Vélu's like formula for computing isogenies on abelian varieties (1h). Séminaire Arithmétique et Théorie de l'Information, November 2009, Marseille.
- An efficient computation of the commutator pairing (20min). ANR Chic, October 2009, Paris.
- A Vélu's like formula for computing isogenies on abelian varieties (40min). ANR Chic, October 2009, Paris.
- Computing isogenies of small degrees on abelian varieties (20min). Journées d'arithmétiques 2009, July 2009, Saint-Etienne.
- Computing isogenies of small degrees on abelian varieties (1h). Séminaire de cryptographie, April 2009, Rennes.

- Abelian varieties and isogenies (30min). Tsukuba Cryptographic Seminar, November 2008, Tsukuba, Japan.

## Rump Sessions

- Finding a supersingular isogeny path with only one isogeny computation (4 min). Eurocrypt 2023, April 2023, Lyon, France. (Video.)
- Sleeping in the volcano. ECC 2011 conference, September 2011, Nancy.
- AVIsogenies, a library for computing isogenies between abelian varieties, with Gaëtan Bisson, Romain Cosset. ECC 2010, October 2010, Redmond, USA. (Video link (starts at 16m30s).)

## Workgroup

April 2018 — Huang's proposal for trilinear maps.

## Vulgarization

April 2023 — Enchainer des blocs à la chaîne. Podcast Désassemblons le numérique - Épisode 6.

November 2022 — Les enjeux de la blockchain écologique (5min). Plenary session, FrenchTech, Bordeaux.

September 2022 — Emmanuel Jeannot, Damien Robert, Les Cryptomonnaies et les NFT (1h). Unithé ou Café, Inria Bordeaux.

February 2020 — Cryptologie, la science des secrets. Présentation grand public, Médiathèque de Mériadeck, Bordeaux.

November 2017, December 2018, December 2019 — Informal discussion about cryptography with students from ENS Lyon..

October 2018 — Animation on cryptography and poster presentation for the « Journée Porte Ouverte » of Inria Bordeaux.

October 2018 — Panorama des mathématiques de la cryptologie. Presentation for the students of the Lycée Montaigne.

September 2018 — Animation on cryptography and poster presentation for the ten years Inria Bordeaux celebration.

May 2018 — Panorama des mathématiques de la cryptologie. Presentation for the laureates of Alkindi.

September 2017 — Panorama des mathématiques de la cryptologie. Presentation for the students of the ESME Sudria school.

June 2017 — Panorama des mathématiques de la cryptologie. Presentation for the laureates of Alkindi.

May 2016 — Panorama des mathématiques de la cryptologie. Presentation for the laureates of Alkindi.

January 2016 — Presentation of cryptography for ENS Rennes students. Introduction, Elliptic curve cryptography,

2015 — Informal discussion about cryptography with students from ENS Rennes..

March 2015 — Discussion with the public about the movie Imitation Game on the role of Alain Turing in Computer Science and Cryptography , Bordeaux.

April 2014 — Algorithmic number theory and cryptography (30min). Team presentation for the director of Inria Bordeaux, Inria Bordeaux.

December 2013 — Algorithmic number theory and cryptography (30min). Presentation of my research themes to the Inria Bordeaux Scientific commitee, Inria Bordeaux.

2012 – 2013 — Writing articles for Sonews, the internal paper of the research center Inria Bordeaux., Bordeaux.

April 2013 Petit panorama des mathématiques de la cryptologie. Presentation for the students in Mines de Nancy, Labri, Bordeaux.

February 2012 Panorama de la cryptographie sur les courbes elliptiques. Lorraine Phd prize ceremony, Conseil général de Lorraine, Metz. More info.

June 2011 Students meeting Aquitec 2011, Bordeaux.

## Activities Slides

FAST — (Harder Better) FAster STronger Cryptography (10 min). Review of joint teams.

CIAO — Cryptography, Isogenies and Abelians varieties (10 min). Administrative overview for the kickoff meeting.

CIAO — Cryptography, Isogenies and Abelians varieties (10 min). Administrative meeting for the ANR projects.

March 2019 Modular polynomials for abelian surfaces (10 min). Lfant evaluation seminar.

September 2018 FAST — (Harder Better) FAster STronger Cryptography (30 min). Evaluation seminar of the Lirima laboratory, Paris.

May 2015 MACISA — Mathematics applied to cryptology and information security in Africa (30 min). Lirima team leaders meeting, Saint-Louis, Sénégal.

September 2014 MACISA — Mathematics applied to cryptology and information security in Africa (30 min). Evaluation seminar of the Lirima laboratory, Paris.

August 2014 Bordeaux 2016: A canonical choice for ANTS XII (15 min). Presentation to host ANTS XII in Bordeaux, GyeongJu, Korea.

September 2013 MACISA — Mathematics applied to cryptology and information security in Africa (30min). Presentation of the MACISA team for the Lirima days, Rabat, Maroc.

## Patents

- Kristin Lauter, Damien Robert, Computing genus 2 curves using general isogenies. May 2014.

## Foreign stays and conferences attended

April 2023 Eurocrypt 2023, Lyon, France.

September 2018 Evaluation seminar of the Lirima laboratory, Paris.

December 2015 Seminar on security of the Colloque de Recherche en Informatique (CRI 2015), Université Yaoundé I, Cameroun.

October 2015 Journées C2 Codage et Cryptographie, La Londe-Les-Maures.

September 2015 Elliptic Curves Cryptography (ECC 2015) Summer School, Bordeaux.

September 2015 Modular Forms and Curves of Low Genus: Computational Aspects, ICERM, Providence, USA.

May 2015 Lirima team leaders meeting, Saint-Louis, Sénégal.

March 2015 École Mathématique Africaine, Franceville, Gabon.

October 2014 Elliptic Curves Cryptography (ECC 2014), Chennai, India.

September 2014 Evaluation seminar of the Lirima laboratory, Paris.

August 2014 International Algorithmic Number Theory Symposium (ANTS-XI), GyeongJu, Korea.

August 2014 International Congress of Mathematicians (ICM 2014), Seoul, Korea.

June 2014 ANR Peace conference Effective moduli spaces and applications to cryptography, Rennes.

May 2014 Discrete Logarithm Problem Conference DLP 2014, Ascona, Suisse.

| | |
|---|---|
| March 2014 | Journées C2 Codage et Cryptographie, Grenoble. |
| October 2013 | Geometry and Cryptography (Geocrypt 2013), Tahiti. |
| September 2013 | Journées du Lirima, Rabat, Maroc. |
| August 2013 | One week visit to Microsoft Research, Redmond, USA. |
| August 2013 | Selected Area in Cryptography (SAC 2013), Simon Fraser University, Canada. |
| June 2013 | Arithmetic Geometry Cryptography and Coding Theory (AGCT 14), Luminy, Marseille. |
| May 2013 | One week visit to EPFL, Lausanne. |
| January 2013 | Pari/GT Workshop, Bordeaux. |
| October 2012 | Journées C2 Codage et Cryptographie, Dinard. |
| August 2012 | One week visit to Microsoft Research, Redmond, USA. |
| July 2012 | International Algorithmic Number Theory Symposium (ANTS-X), San Diego, USA. |
| September 2011 | Elliptic Curves Cryptography (ECC 2011) and Summer School, Nancy. |
| June 2011 | Geometry and Cryptography (Geocrypt 2011), Bastia. |
| April 2011 | Journées C2 Codage et Cryptographie, Oléron. |
| December 2010 | Algorithmics of L-functions workshop, Bordeaux. |
| October 2010 | Elliptic Curves Cryptography (ECC 2010), 25 year anniversary of elliptic curves computation, Redmond, USA. |
| July 2010 – September 2010 | Three month Microsoft Research Internship in the cryptographic team to work on genus 2 class polynomials with Kristin Lauter, Redmond, USA. |
| July 2010 | International Algorithmic Number Theory Symposium (ANTS-IX), Nancy. |
| May 2010 | Conférence Algorithmique et Arithmétique avec applications à la cryptographie, Moscow, Russia. |
| October 2009 | Elliptic Curves Cryptography (ECC 2009), Calgary. |
| July 2009 | Journées d'arithmétiques 2009, Saint-Etienne. |
| March 2009 | Arithmetic Geometry Cryptography and Coding Theory (AGCT), Luminy. |
| November 2008 | Three weeks visit at Tsukuba University in the team of professor Okamoto to work on pairings, Tokyo. |
| October 2008 | CADO workshop on integer factorisation, Nancy. |
| July 2008 | International Algorithmic Number Theory Symposium (ANTS-VIII), Banff, Canada. |
| June 2008 | Crypto week, LIX, Saclay.. |
| April 2008 | École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Marseille. |
| June 2007 | LLL+25, Caen. |
| March 2007 | École Jeunes chercheurs en informatique mathématique (EJCIM, GDR IM), Nancy. |
| February 2007 | Journées nationales du calcul formel, Luminy. |
| April 2006 | Théorie géométrique et cohomologie des groupes: rigidité et déformations (Summer school), Luminy. |